UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/660,300	09/12/2000	Robert Hugh Smithson	NAI1P154/99.078.01	6946

28875 7590 07/13/2004

SILICON VALLEY INTELLECTUAL PROPERTY GROUP
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	PAPER NUMBER
2131	8

DATE MAILED: 07/13/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/660,300	**Applicant(s)** SMITHSON ET AL.	
	Examiner Christopher A. Revak	**Art Unit** 2131	

-- ***The MAILING DATE of this communication appears on the cover sheet with the correspondence address*** --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 April 2004*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-13,15-25 and 27-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-13,15-25,27-36* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed April 22, 2004 have been fully considered but they are not persuasive.

The applicant has argued that a prima facie case of obviousness has no been met by then previous dependent claims 2,14, and 26 being incorporated into independent claims 1,13, and 25 respectively. The examiner respectfully disagrees. Shieh discloses of "defining abnormal limits to determine abnormal process behavior" as is recited in column 17, lines 17-30. Broadly interpreting the teachings of Chen, it can be interpreted that this can include "determining how many e-mail messages are sent having an identical message title" since this is considered an abnormal process behavior. Please refer to the rejection as is recited below.

The examiner contends that no official notice is taken in regards to "determining how many e-mail messages are sent having an identical message title", but is rather broadly interpreting the claim limitations versus the teachings of Chen et al.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1,3-7,13,15-19,25, and 27-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shieh et al in view of Arnold et al in view of Chen et al.

As per claims 1, 13, and 25, Shieh teaches a computer program product/method for detecting an outbreak of a virus on a computer apparatus, said computer program product/method comprising:

(i) measuring one or more measurement parameters indicative of non-virus specific activity of said computer apparatus over a respective measurement period, see col. 17, lines 17-30.

(ii) comparing said one or more measurement parameters with respective predetermined threshold levels, see col. 17, lines 17-30.

Shieh fails to explicitly disclose (iii) generating a signal indicative of an outbreak of a computer virus if one or more of said one or more measurement parameters crosses a respective predetermined threshold level.

However, Arnold in an analogous art, teaches this limitation, see col. 22, lines 62-68, and col. 24, lines 12-15. It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the feature of sending an alert upon possible detection of a virus as taught by Arnold with the event that some thresholds were breached in the Shieh invention. One would have been motivated to do so because an alert would notify the user/administrator of the system, so that correct action could be taken to remedy the possible virus problem.

The Shieh-Amold combination teaches all limitations of the base claims, but fails to explicitly teach wherein one of said measurement parameters is how many e-mail messages are sent having an identical message title/file attachment/attachment of a given file type. Shieh however does teach in regards to detecting/preventing an unknown virus from propagating, monitoring its pattern according to his teaching based on several threshold parameters. Shieh further teaches that these parameters are used for "defining limits to determine abnormal process behavior." See col. 17, lines 17-30.

Chen in an analogous art teaches that e-mail attachments are of particular concern in relation to the transmission of computer viruses. Chen further mentions that these attachments may contain executable files. Chen also teaches that an attachment to an email message may contain a file infected with a computer virus. Chen says that an email having a virus attachment may be broadcast over a network. In light of this teaching of Chen it would have been obvious to one having ordinary skill in the art at the time the invention was made to include as parameters in the Shieh-Arnold combination, threshold parameters such as those taught by Chen. Namely, because Chen teaches the danger of email attachments in association with viruses, and specifically teaches that should an email be broadcast, it may infect multiple recipients, it would have been obvious to one having ordinary skill in the art to monitor all characteristics of a broadcast email. Specifically these threshold parameters would include email subject line, since a broadcast email would have the same subject line. Similarly these parameters could further include file attributes, such as file attachment size, name, or type. One would have been motivated to do so because Chen teaches that email attachments pose a potential virus risk, and therefore one would want to monitor this type of email activity. See col. 3, lines 17-32.

As per claims 3-5, 15-17, and 27-29, the Shieh-Amold combination teaches all limitations of the base claims, but fails to explicitly teach wherein one of said measurement parameters is how many e-mail messages are sent having an identical message title/file attachment/attachment of a given file type. Shieh however does teach in regards to detecting/preventing an unknown virus from propagating, monitoring its pattern according to his teaching based on several threshold parameters. Shieh further teaches that these parameters are used for "defining limits to determine abnormal process behavior." See col. 17, lines 17-30.

Chen in an analogous art teaches that e-mail attachments are of particular concern in relation to the transmission of computer viruses. Chen further mentions that these attachments may contain executable files. Chen also teaches that an attachment to an email message may contain a file infected with a computer virus. Chen says that an email having a virus attachment may be broadcast over a network. In light of this teaching of Chen it would have been obvious to one having ordinary skill in the art at the time the invention was made to include as parameters in the Shieh-Arnold combination, threshold parameters such as those taught by Chen. Namely, because Chen teaches the danger of email attachments in association with viruses, and specifically teaches that should an email be broadcast, it may infect multiple recipients, it would have been obvious to one having ordinary skill in the art to monitor all characteristics of a broadcast email. Specifically these threshold parameters would include email subject line, since a broadcast email would have the same subject line. Similarly these parameters could further include file attributes, such as file attachment size, name, or type. One would have been motivated to do so because Chen teaches that email attachments pose a potential virus risk, and therefore one would want to monitor this type of email activity. See col. 3, lines 17-32.

As per claims 6, 18, and 30, Shieh further teaches wherein one of said measurement parameters is e-mail throughput within said computer system, see col. 4, lines 45-59, in which Shieh teaches pattern-oriented Intrusion detection, which helps define patterns of object privilege and data flows that characterize operational security problems in otherwise secure systems.

As per claim 7, 19, and 31, examiner respectfully asserts that it is well known in the art that in order to calculate throughput of e-mails, one would multiply the number of emails by the total size.

As per claims 3-5, 15-17, and 27-29, the Shieh-Amold combination teaches all limitations of the base claims, but fails to explicitly teach wherein one of said measurement parameters is how many e-mail messages are sent having an identical message title/file attachment/attachment of a given file type. Shieh however does teach in regards to detecting/preventing an unknown virus from propagating, monitoring its pattern according to his teaching based on several threshold parameters. Shieh further teaches that these parameters are used for "defining limits to determine abnormal process behavior." See col. 17, lines 17-30.

Chen in an analogous art teaches that e-mail attachments are of particular concern in relation to the transmission of computer viruses. Chen further mentions that these attachments may contain executable files. Chen also teaches that an attachment to an email message may contain a file infected with a computer virus. Chen says that an email having a virus attachment may be broadcast over a network. In light of this teaching of Chen it would have been obvious to one having ordinary skill in the art at the time the invention was made to include as parameters in the Shieh-Arnold combination, threshold parameters such as those taught by Chen. Namely, because Chen teaches the danger of email attachments in association with viruses, and specifically teaches that should an email be broadcast, it may infect multiple recipients, it would have been obvious to one having ordinary skill in the art to monitor all characteristics of a broadcast email. Specifically these threshold parameters would include email subject line, since a broadcast email would have the same subject line. Similarly these parameters could further include file attributes, such as file attachment size, name, or type. One would have been motivated to do so because Chen teaches that email attachments pose a potential virus risk, and therefore one would want to monitor this type of email activity. See col. 3, lines 17-32.

4. Claims 8,9,20,21,32, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shieh et al in view of Arnold et al in further view of Chen et al in further view of Lubarksy.

As per claims 8-9, 20-21, and 32-33, the Shieh-Arnold-Chen combination teaches all limitations of the base claims, but fails to explicitly disclose said respective predetermined threshold levels are varied in dependence upon time of day/day of week. However, Lubarsky in an analogous art adequately teaches that the normal quantity of traffic on a network varies from day to day and at different times of the day. See Col. 1 line 32-41. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to set different (i.e. lower) thresholds during off-peak hours. One would have been motivated to do so because this would reduce the problem of having false positives in which an indication of a possible virus outbreak is given when in fact the activity triggering this alarm is completely characteristic and normal for a given instance.

5. Claims 10-12,22-24, and 34-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shieh et al in view of Arnold et al in further view of Chen et al in further view of Walsh et al.

As per claims, 10-12, 22-24, and 34-36, the Shieh-Arnold-Chen combination teaches all limitations of the base claims, but fails to explicitly disclose that's the features of the virus protection system/method/software program are user definable/selectable. However, Walsh in an analogous art adequately discloses user selectable features within virus-protection software, see col. 3, lines 20-41. It would have been obvious to one having ordinary skill in the art at the time the invention was made to make the features that are available in the Shieh-Arnold-Chen combination user-selectable as taught by Walsh. One would have been motivated to do so because this would allow for added versatility to the software, making it specialized for any given consumer, making the product more marketable.

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 703-305-1843. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CR
CM
July 2, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100